

DEPLOYMENT GUIDE

Integrating BloxOne Threat Defense TIDE IoC into Cisco Firepower Management Center



TABLE OF CONTENTS

Introduction	3
Requirements	3
BloxOne Threat Defense Configuration Instructions	3
Cisco Threat Intelligence Director Configuration Instructions	5
Viewing Status and Data	7

Introduction

Cisco Firepower Management Center manages the following Cisco network security solutions:

- Firepower Next-Generation Firewall
- Firepower Next-Generation IPS
- ASA with FirePOWER Services
- FirePOWER Threat Defense for ISR
- Advanced Malware Protection (AMP) for Networks

A [Cisco Firepower Management Center](#) feature, Threat Intelligence Director, ingests third-party threat feeds and correlates enriched observations from Cisco security solutions to detect and alert on security incidents. By converting intelligence into actionable indicators of compromise, you can block or monitor more threats, reduce the number of alerts you must review, and improve your overall security posture.

This deployment guide shows you how to upload the Infoblox BloxOne Threat defense TIDE feeds into Threat Intelligence Director.

Requirements

- Access to BloxOne Threat Defense TIDE.
- Cisco Firepower Management Center version 6.2.2 or above.

BloxOne Threat Defense Configuration Instructions

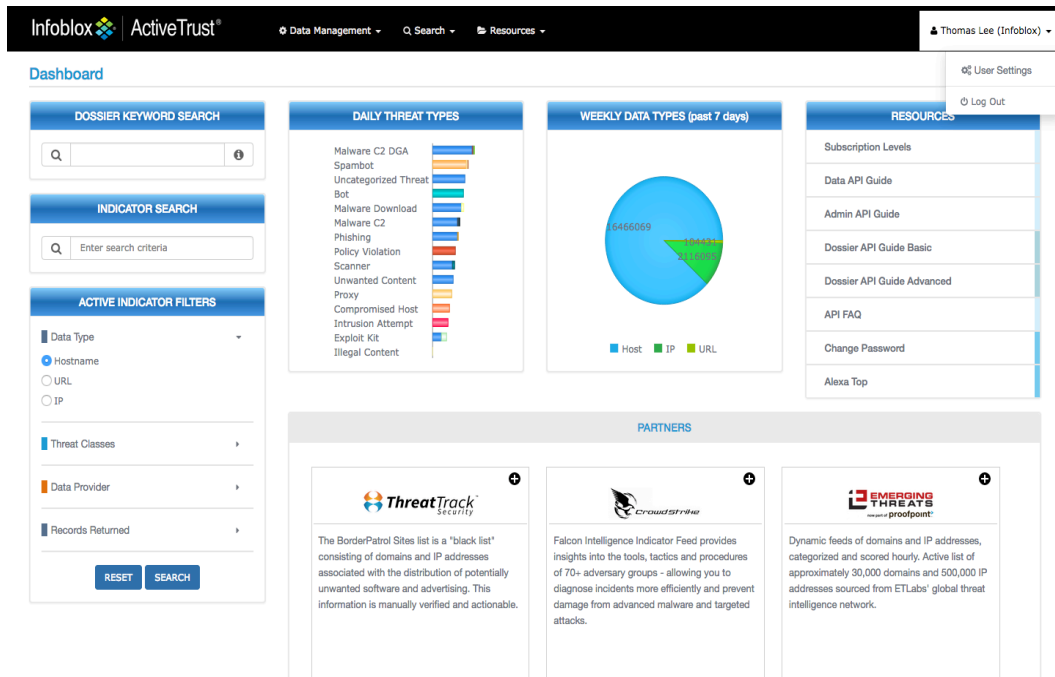
1. Log into the BloxOne website. We will be assigning the API key to access the threat feeds.

The screenshot displays the Infoblox ActiveTrust dashboard. The top navigation bar includes the Infoblox logo, ActiveTrust branding, and menu items for Data Management, Search, and Resources. The user is identified as Thomas Lee (Infoblox).

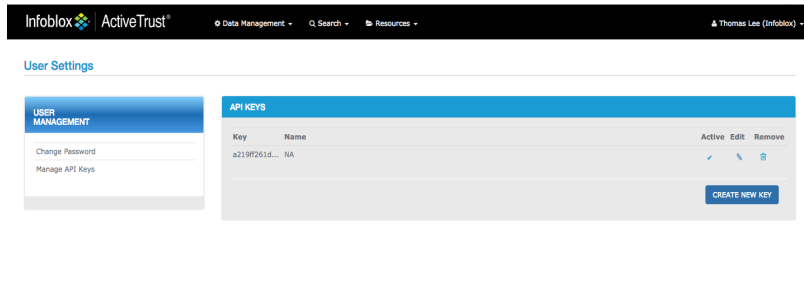
The dashboard is divided into several sections:

- DOSSIER KEYWORD SEARCH:** A search bar with a magnifying glass icon and a help icon.
- INDICATOR SEARCH:** A search bar with the placeholder text "Enter search criteria".
- ACTIVE INDICATOR FILTERS:** A sidebar with filters for Data Type (Hostname selected, URL, IP), Threat Classes, Data Provider, and Records Returned. It includes RESET and SEARCH buttons.
- DAILY THREAT TYPES:** A horizontal bar chart showing the frequency of various threat types over the last 24 hours. The most prominent categories are Malware C2 DGA, Spambot, and Uncategorized Threat.
- WEEKLY DATA TYPES (past 7 days):** A pie chart showing the distribution of data types. The largest segment is Host (6456069), followed by IP and URL.
- RESOURCES:** A list of links to various guides and tools, including Subscription Levels, Data API Guide, Admin API Guide, Dossier API Guide Basic, Dossier API Guide Advanced, API FAQ, Change Password, and Alexa Top.
- PARTNERS:** A section featuring three partner cards: ThreatTrack Security, CrowdStrike, and EMERGING THREATS (a part of proofpoint). Each card provides a brief description of the partner's threat intelligence feed.

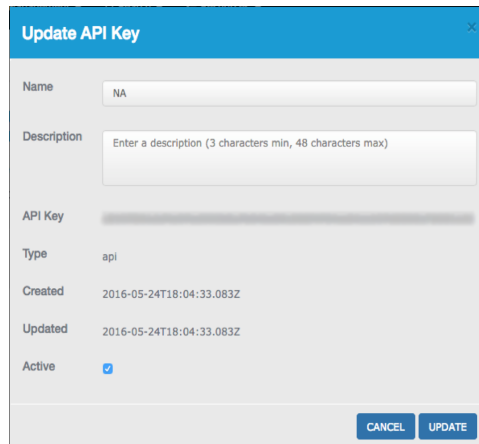
2. In the upper right corner of the screen, click on the username and select User Settings.



3. Click on Manage API Keys on the left side.



4. Click on the Edit button and copy the API key to your clipboard. Click Cancel to close this window.



5. Refer to the Dossier and TIDE quick start guide to assign the API key and creation of URLs.

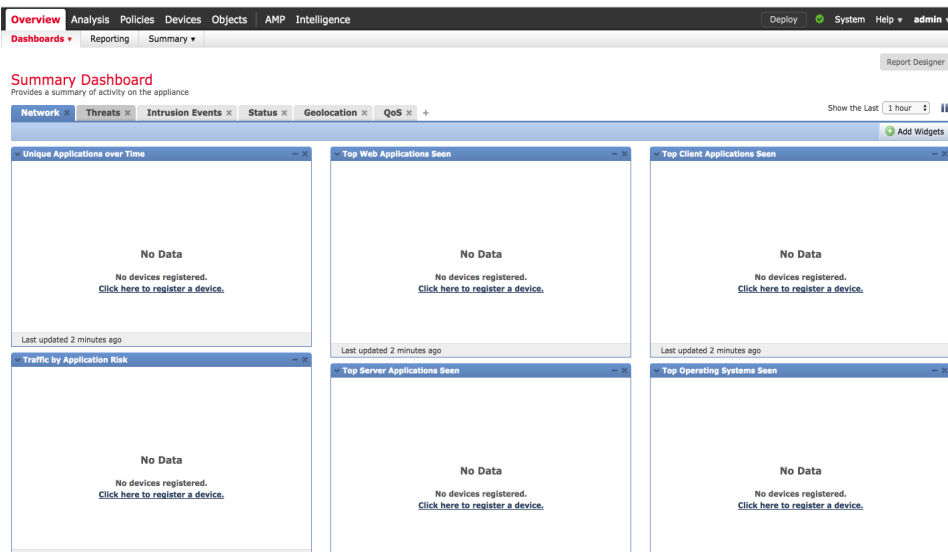
Cisco Threat Intelligence Director Configuration Instructions

1. In this example, you will need to create three request URLs: one for bad hosts, bad IPs, and bad URLs. They will look similar to the following:

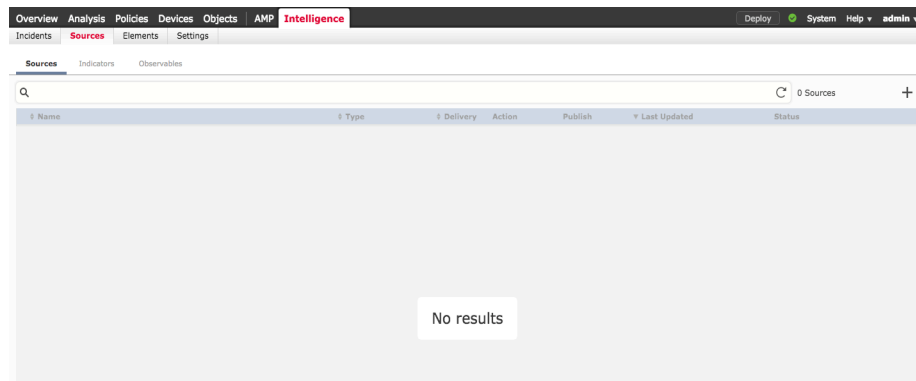
- a. **host:** `https://<api key>
@platform.activetrust.net:8000/api/data/threats/host?data_format=stix&rlimit=1000`
- b. **IP:** `https://<api key>
@platform.activetrust.net:8000/api/data/threats/ip?data_format=stix&rlimit=1000`
- c. **URL:** `https://<api key>
@platform.activetrust.net:8000/api/data/threats/url?data_format=stix&rlimit=1000`

2. To complete the request URLs above, you will need to prepend your user-specific API key and add an @ before the word platform. You will need to add the type of data before the ?data_format word. In the cases above, the types of data are: host, ip, and url. Lastly, you can adjust the number of records downloaded from the feed by modifying the limit value at the end of the URL. Refer to the filtering fields within the threat API section for additional ways filtering the feeds.

3. Login to the Cisco Firepower Management Center.



4. Navigate to the Intelligence → Sources.



5. Click on the + button to add a source.

The 'Add Source' dialog box shows the following configuration:

- DELIVERY: TAXII (selected), URL, Upload
- URL: [Empty field]
- SSL Settings: [Dropdown arrow]
- USERNAME: [Empty field]
- PASSWORD: [Empty field]
- FEEDS: Select feeds... [Dropdown arrow]
- Note: A separate source will be added for each feed selected. The name will default to the name of the feed and can be edited later.
- ACTION: Monitor [Selected]
- UPDATE EVERY (MINUTES): 1440 [Input field], Never Update [Unchecked checkbox]
- TTL (DAYS): 90 [Input field]
- PUBLISH: [Checked toggle]
- Buttons: Save, Cancel

6. Click on the URL delivery button, enter one of the three URLs that are similar to the ones listed in step 1, enter the name of the source, enter a comment, and change the update time if you wish. 60 minutes is the minimum time. Click Save when done.

The 'Add Source' dialog box shows the following configuration:

- DELIVERY: TAXII, URL (selected), Upload
- TYPE: STIX [Dropdown arrow]
- URL: [Empty field]
- SSL Settings: [Dropdown arrow]
- NAME: hosts [Input field]
- DESCRIPTION: from Infoblox [Text area]
- ACTION: Monitor [Selected]
- UPDATE EVERY (MINUTES): 60 [Input field], Never Update [Unchecked checkbox]
- TTL (DAYS): 90 [Input field]
- PUBLISH: [Checked toggle]
- Buttons: Save, Cancel

7. Repeat the above step to add IP and host feeds. When done the intelligence source should look like the following:

Name	Type	Delivery	Action	Publish	Last Updated	Status
URLs from Infoblox	STIX	URL	Monitor	[Checked]	3 minutes ago Pause Updates	Completed
hosts from Infoblox	STIX	URL	Monitor	[Checked]	17 minutes ago Pause Updates	Completed
IPs from Infoblox	STIX	URL	Monitor	[Checked]	31 minutes ago Pause Updates	Completed

Viewing Status and Data

1. Hover over one of the Completed links to get the download status.

The screenshot shows the 'Sources' page in the Cisco Firepower Management Center. A dropdown menu is open over the 'Completed' status of a source, displaying the following information:

- Status Message: Operation completed successfully
- Last Updated: 7 minutes ago
- Next Update: tomorrow
- Total Indicators: 10
- Consumed: 10
- Discarded: 0
- Observables: 2
- Unsupported: 0
- Invalid: 0

2. Click on the Observables tab to view the IoCs downloaded.

The screenshot shows the 'Observables' page in the Cisco Firepower Management Center. The page displays a list of indicators with the following columns: Type, Value, Indicators, Action, Publish, Updated At, and Expires. The list includes various URLs and IP addresses.

Type	Value	Indicators	Action	Publish	Updated At	Expires
URL	www.logicbeam.xyz/f11h8Z620c0*kOKmnjIFkmjKvy0Mjh383/t/hot/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
URL	www.logicbeam.xyz/a25nk8520_c3kOKmnjIFkmjKvy0Mjh59H/hot/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
URL	www.logicbeam.xyz/money/1d4n8y620c1kOKmnjIFkmjKvy0Mjh10/21/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
URL	www.logicbeam.xyz/c9bzm2862F0c1qkOKmnjIFkmjKvy0Mjh10e/often/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
URL	www.logicbeam.xyz/62986GyB20c0kOKmnjIFkmjKvy0Mjh725/often/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
URL	www.logicbeam.xyz/ef3rN7a25u0c2kOKmnjIFkmjKvy0Mjha50/his/3/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
URL	regent.organicmarket.com/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
URL	udn.com/news/story/7254/2498020?from=udn-catelistnews_ch2/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
URL	shyness.globalpharmacytrade.com/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
URL	atmosphere.xn--b1ah5aek6bbi.xn--p1ai/	1	Monitor	On	Aug 10, 2017 6:15 PM EDT	Nov 8, 2017 5:15 PM EST
IPv4	24.252.215.132	1	Monitor	On	Aug 10, 2017 5:47 PM EDT	Nov 8, 2017 4:47 PM EST
IPv4	66.171.229.61	1	Monitor	On	Aug 10, 2017 5:47 PM EDT	Nov 8, 2017 4:47 PM EST
IPv4	24.252.213.162	1	Monitor	On	Aug 10, 2017 5:47 PM EDT	Nov 8, 2017 4:47 PM EST
IPv4	66.171.229.60	1	Monitor	On	Aug 10, 2017 5:47 PM EDT	Nov 8, 2017 4:47 PM EST

3. You can also search specific IoCs like an IP range. For example, set the type to IPv4 and set a value to 109.67. You may see the following:

The screenshot shows the 'Observables' page in the Cisco Firepower Management Center with search filters applied. The search filters are set to Type: IPv4 and Value: 109.67. The resulting list of observables is as follows:

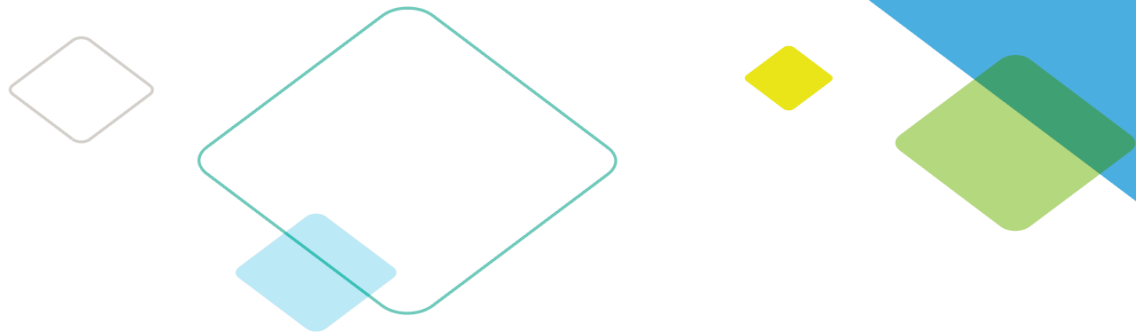
Type	Value	Indicators	Action	Publish	Updated At	Expires
IPv4	109.67.179.206	1	Monitor	On	Aug 10, 2017 5:47 PM EDT	Nov 8, 2017 4:47 PM EST
IPv4	109.67.2.67	1	Monitor	On	Aug 10, 2017 5:47 PM EDT	Nov 8, 2017 4:47 PM EST

4. Click on one of the Indicators link to see that the IoC is related to an Indicator for a spambot.

Type	Name	Source	Incidents	Action	Publish	Last Updated	Status
IPv4	Spambot - Spambot_Slenbot	IPs		Monitor	<input checked="" type="checkbox"/>	Aug 10, 2017 5:47 PM EDT	Completed

5. Click on the Source link and the screen shows you the source for the Indicator, which in this case is the BloxOne Threat Defense TIDE IP feed you configured above.

Name	Type	Delivery	Action	Publish	Last Updated	Status
IPs <small>from Infoblox</small>	STIX	URL	Monitor	<input checked="" type="checkbox"/>	44 minutes ago Pause Updates	Completed



Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054

+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com



© 2018 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).